

Appl. No.: 10/561,699  
Amdt. Dated: March 3, 2009  
Reply to Office Action of September 4, 2008

### REMARKS

Claims 1 – 45 were originally pending in the present application. However, Claims 39 and 43 have been cancelled and Claims 46 – 52 have been added, leaving Claims 1 – 38, 40 – 42, and 44 – 52 pending and at issue.

Reconsideration of the rejections, in light of the aforesaid amendments and present remarks, is respectfully requested. The present amendments have been entered for the purpose of placing the application into a proper condition for allowance.

In the claims, amendment has been made to independent Claims 1 and 19 to make clear that the financial institution application is holding an account of the customer from which payment is to be made.

In addition, new dependent claims have been added to make clear that the financial institution application may be an Internet banking application, for example, such as those that are already commonly known. Support for these additional claims may be found throughout the specification.

Dependent claims have been added to the feature that the financial institution application may be connected to the customer computing system in order to obtain the security means. This is also clearly supported in the specification, see particularly the example where a customer computer is connected to an Internet banking application.

Claims 36 and 40 have been amended as well. The amendments include the features that the connection between a financial institution application and a computing system is implemented so that the computing system may provide the security means to the financial institution application. The amendments also includes the features that the financial institution

Appl. No.: 10/561,699  
Amdt. Dated: March 3, 2009  
Reply to Office Action of September 4, 2008

application holds an account of the payor from which payment is to be made. Similar dependent claims have been added to the financial institution being an Internet banking application.

Regarding the Examiner's objection under 35 USC 101, the present independent method claims have been amended to add the limitation "utilizing the obtained security means during the transaction to protect the customer's account." Applicant contends the recitation of the utilization of the security means to protect the customer's account is sufficient to tie the method to statutory subject matter. Claims 19 and 40 have been so amended.

Regarding the Examiner's rejections to other claims on the basis of the prior art document to Swain (WO 02/25604), Applicant traverses the rejections and requests reconsideration in light of the following remarks.

With regard to independent Claims 1 and 19 and their dependent claims, Applicant respectfully submits that the claims as now amended are novel and inventive over the disclosure of Swain.

A problem with prior art systems for implementing transactions over computing systems, such as shopping over the Internet utilizing credit cards and secure interfaces such as SSL, is that a person shopping on a network such as the Internet must provide personal account details, such as a credit card number, to a third party who they do not know and who may not be trustworthy. In most cases, this third party is a merchant. This problem may be addressed by direct debit from a customer's account, but this requires authority from the customer and is therefore not viable for all on-line shopping. These problems are discussed in detail in the "Background of the Invention" section of the specification of the present application.

The present invention, however, allows a user to transfer money from a user account to a merchant account during on-line shopping without having to provide any secure information to

Appl. No.: 10/561,699  
Amdt. Dated: March 3, 2009  
Reply to Office Action of September 4, 2008

the merchant. This is achieved by the step of, during the on-line transaction, implementing a connection to enable the user to provide a financial institution application with their security means (e.g. password) via their own computing system. In the preferred embodiment, the system operates to directly connect the user's computing system to the financial application during the on-line transaction with the merchant. The customer deals directly with their financial institution (e.g. via a bank website) and no secure information needs to be provided to the merchant or any other non-trusted party. The communication is simply between the customer computer and the financial institution application.

In the preferred embodiment, other details apart from the security means are automatically provided to the financial institution application, eg. merchant ID number, merchant account number, payment amount, etc.

The prior art does not operate in this way. In Swain, there is no connection implemented between a customer computer and a financial institution application during the on-line transaction with the merchant, to enable the customer to provide account details, passwords, etc directly to the financial institution application.

Swain discloses a system where security means such as client payment information such as credit card numbers are stored on a separate third party 'client wallet server'. A "unifying interface" is arranged to obtain the payment details (credit card details) from the client wallet server, obtain the transaction details from the merchant and then to interact with a financial system in order to prosecute the transaction. The unifying interface is provided by a "merchant wallet server (MWS)". See pages 6 and 7 of Swain. See in particular page 6 lines 7 to 10, where it is made clear that the "security means", such as credit card information and the like, is stored in an electronic wallet on the client wallet server 130. Referring to Figure 1 of the drawings, it is

Appl. No.: 10/561,699  
Amdt. Dated: March 3, 2009  
Reply to Office Action of September 4, 2008

quite clear that the device associated with the card holder 120 is a separate device e.g. a separate "customer computing system".

It is important to note that the transaction is still controlled by a third party system (the client wallet server and MWS) and that the customer computer is not in control. Credit card details and other important information that is stored on the client wallet server is therefore still open to attack by e.g. hackers attacking the client wallet server to obtain the customer's details.

A major novel feature of the present invention is that it essentially puts the client's computer system in control so that the customer can deal with the transaction and no third party system need be involved. All security means can be stored via the customer computing system or remain in the customer's mind (including passwords to enter the financial institution application number as well as credit card details). This provides greater security to the customer.

This is not disclosed or suggested by Swain.

It is also worth pointing out that, in one embodiment, the present invention facilitates access to already existing financial institution applications, such as Internet Banking sites. For example, the customer computer is connected via the interface to an existing Internet Banking site and the user feeds in their passwords and credit card details to pay the merchant. The cited document, on the other hand, requires the use of digital wallets. The present invention removes this requirement or for the user to pre-register any sort of payment details into any system prior to making a transaction. In one embodiment, the user simply has to have an on-line banking account with any financial institution that the system supports. Millions of users already have such accounts.

Note that the customer computing system of embodiments of the present invention may be any computing system which the customer has access to (see page 17, lines 3 to 6).

Appl. No.: 10/561,699  
Amdt. Dated: March 3, 2009  
Reply to Office Action of September 4, 2008

Essentially, the customer remains in control and does not have to trust any third parties with their security means, such as passwords. This is a major advantage for on-line shopping.

The "interface means" as claimed in the present application, may be any means which can enable a connection such that security means can be obtained via a customer computing system. In one embodiment, it may be a software application, such as a software "agent" that is able to navigate the network and connect the customer computing system and financial institution application. In other embodiments, it may be a "link" which a customer computing system can activate to connect to the financial institution application.

Regarding amended Claims 36 and 40, these relate to an embodiment of the invention where the connection to the financial institution application is provided by way of a system message. For example, in one embodiment the system message may be an email providing a link which will connect the customer computing system to the financial institution application. The email message may constitute a bill for services, for example, and have been sent to the customer computing system. They click on the link and they are automatically connected to their financial institution application (e.g. Internet banking) and can enter their password to authorize a payment to a third party account (e.g. the entity that sent the message).

For similar reasons as discussed above, this is not disclosed by Swain.

Support for the claim amendments and submissions is given throughout the specification of the present application. See in particular pages 3, 4, 5 and 6.

Appl. No.: 10/561,699  
Amdt. Dated: March 3, 2009  
Reply to Office Action of September 4, 2008

### CONCLUSION

Claims 1 – 38, 40 – 42, and 44 – 52 are currently pending in the present application. Claims 1, 19, 36 and 40 have been substantively amended to place the application in better condition for allowance. The newly amended claims and their respective dependent claims clearly distinguish over the cited references. Reconsideration of all pending claims is respectfully requested.

Should any formalities remain which can be corrected by Examiner's amendment, Applicant requests that the undersigned be contacted by phone in order to expedite the prosecution of the present case.

Respectfully submitted,

By 

Robert W. Diehl  
PTO Reg. No. 35,118  
Seyfarth Shaw LLP  
Attorneys for Assignee  
131 South Dearborn Street  
Suite 2400  
Chicago, Illinois 60603-5577  
312-460-5000  
312-460-7000 (fax)